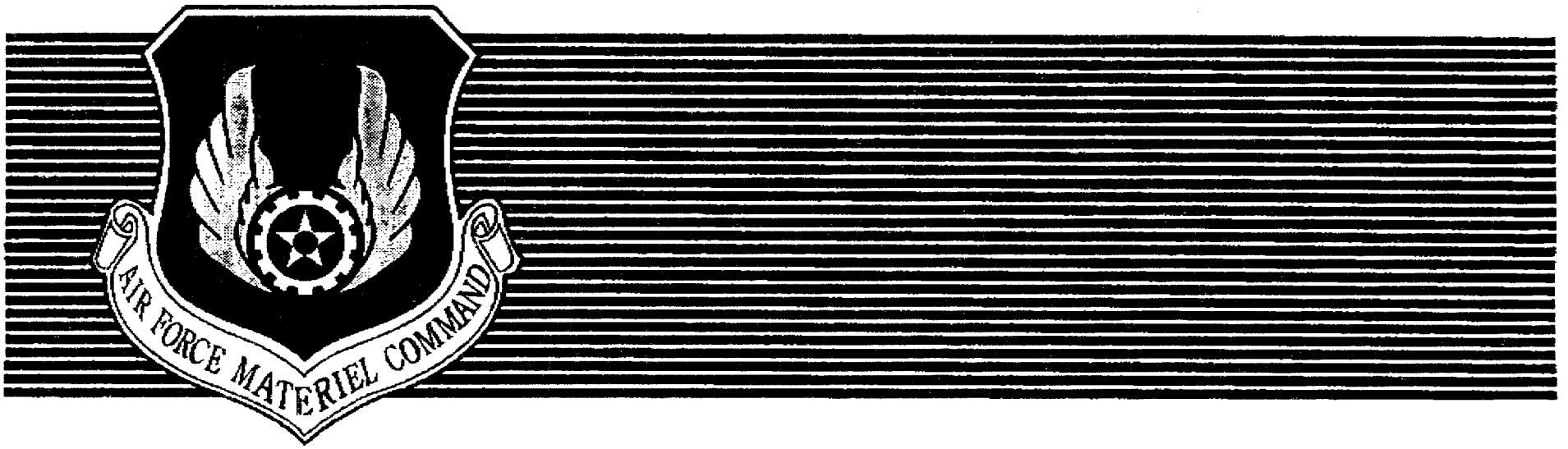


ROME LABORATORY

COMPUTER SECURITY

PRESENTED BY
MR JOSEPH GIORDANO
RL/C3AB
(315) 330-3681

KAMAN SCIENCES-SYR ID:315-472-7241 OCT 11'93 12:14 No.002 P.02

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 11101993	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Rome Laboratory Computer Security	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Rome Laboratory	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms "IATAC COLLECTION"	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 21	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	10/1/95	Briefing

4. TITLE AND SUBTITLE
Rome Laboratory Computer Security

5. FUNDING NUMBERS

6. AUTHOR(S)
Joseph Giordano

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis
Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

The objective of this presentation is to develop & demonstrate theTools & technology necessary to realize trusted c31 systems in Air Force & DoD applications, and to emphasize use of formal Verification to assure Securit/Trust Mechanism Satisfies Formal Security/Trust Policy Model.

14. SUBJECT TERMS
IA

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

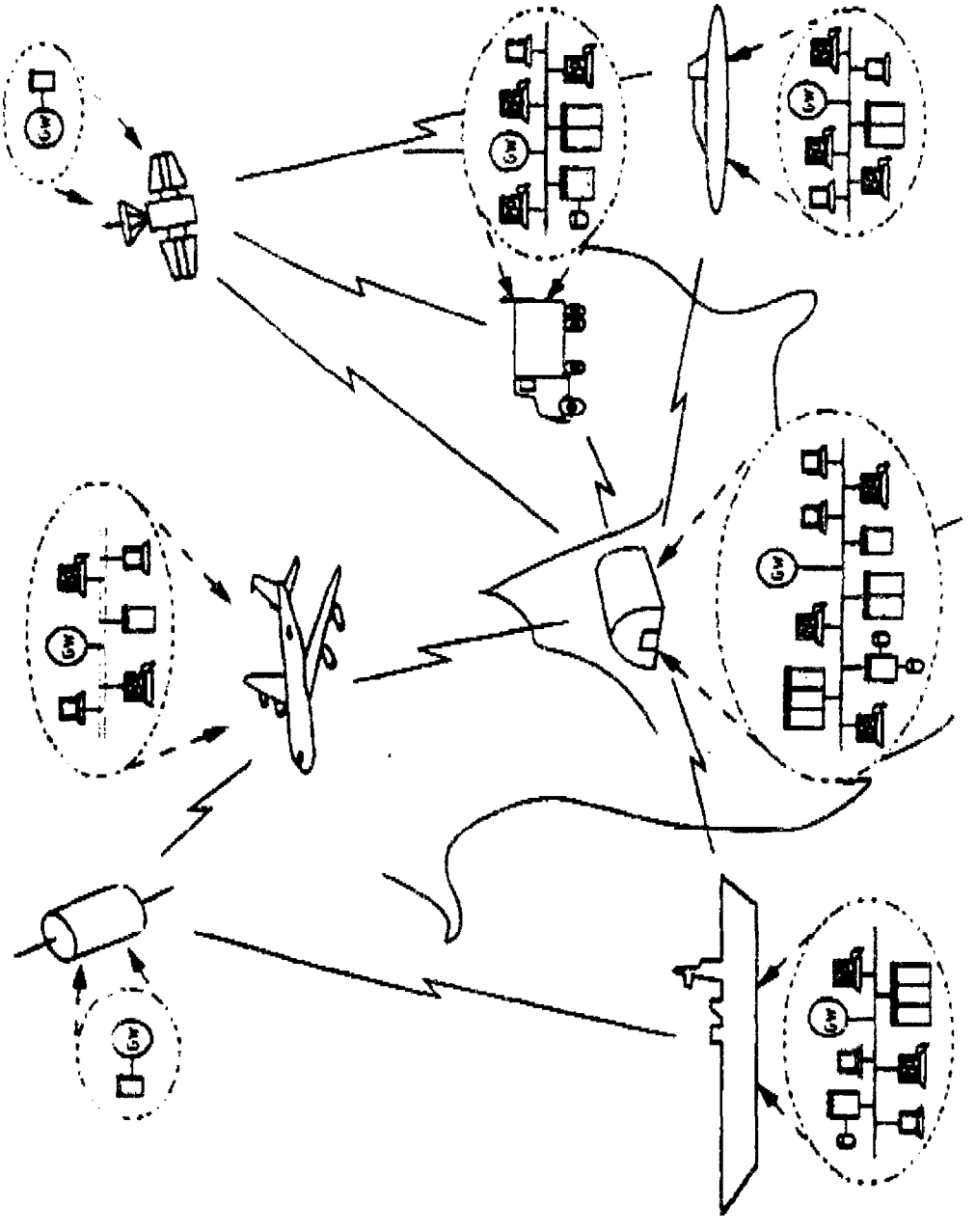
COMPUTERSECURITY

OBJECTIVE: **TO DEVELOP & DEMONSTRATE THE** TOOLS & TECHNOLOGY **NECESSARY TO** REALIZE TRUSTED **C3I** SYSTEMS **IN** AIR FORCE **&** DOD APPLICATIONS

APPROACH: EMPHASIZE **USE** OF FORMAL VERIFICATION **TO** ASSURE **SECURITY/** TRUST MECHANISM SATISFIES **FORMAL** SECURITY/TRUST POLICY MODEL

KAMAN SCIENCES-SYR ID:315-472 7241 OCT 11'93 12:15 No.002 P.03

MULTI LEVEL SECURE C2 SYSTEMS



TECHNOLOGY STATUS

	STATE-OF-THE-ART	DEFICIENCIES
POLICY	ACCESS CONTROL	INTEGRITY ASSURED SERVICE
MECHANISMS	OPERATING SYSTEM GUARDS MULTINET GATEWAY	DISTRIBUTED SYSTEMS DATABASE MGMT SYS PARALLEL PROCESSING
VERIFICATION	TESTING PENETRATION DESIGN VERIFICATION	CODE VERIFICATION TRUSTED COMPILERS TRUSTED HARDWARE SOFTWARE ENGINEERING
CERTIFICATION	AD HOC PROCESS LABOR INTENSIVE	STANDARDIZED PROCESS AUTOMATED TOOLS

COMPUTER SECURITY
AREAS OF INTEREST

- SECURITY PROPERTIES **MODELING**
- **SECURE DISTRIBUTED SYSTEMS**
- MULTILEVEL SECURE DBMS
- FORMAL VERIFICATION
- **CERTIFICATION TECHNOLOGY**

KAMAN SC SYR ID:315-472-7241 OCT 93 12:16 No.002 P.06

SECURITY PROPERTIES MODELING

ROMULUS

ESTABLISHED CONCEPT OF "HOOK-UP" SECURITY

IMPLEMENTED SECURE SYSTEM DEVELOPMENT ENVIRONMENT ON SUN WORKSTATION

POPULATE ENVIRONMENT WITH GENERIC MODELS OF SECURE SYSTEM COMPONENTS

EXTEND ENVIRONMENT TO ADDRESS:
- DATA INTEGRITY
- ASSURED SERVICE

FORMAL MODELS

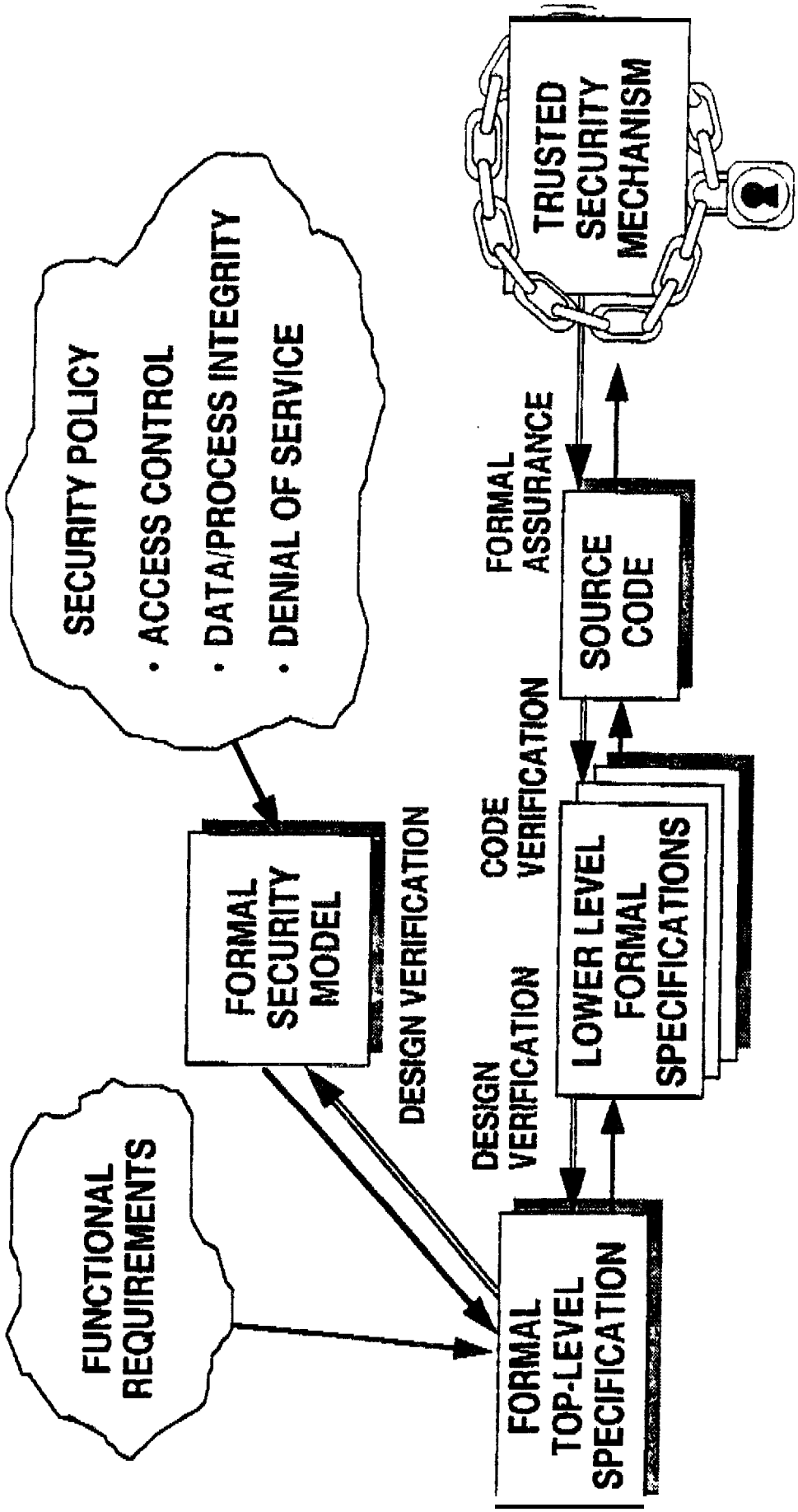
DATABASE INTEGRITY

ASSURED SERVICE FOR DISTRIBUTED SYSTEMS

DATABASE AGGREGATION

DISTRIBUTED SYSTEMS INTEGRITY

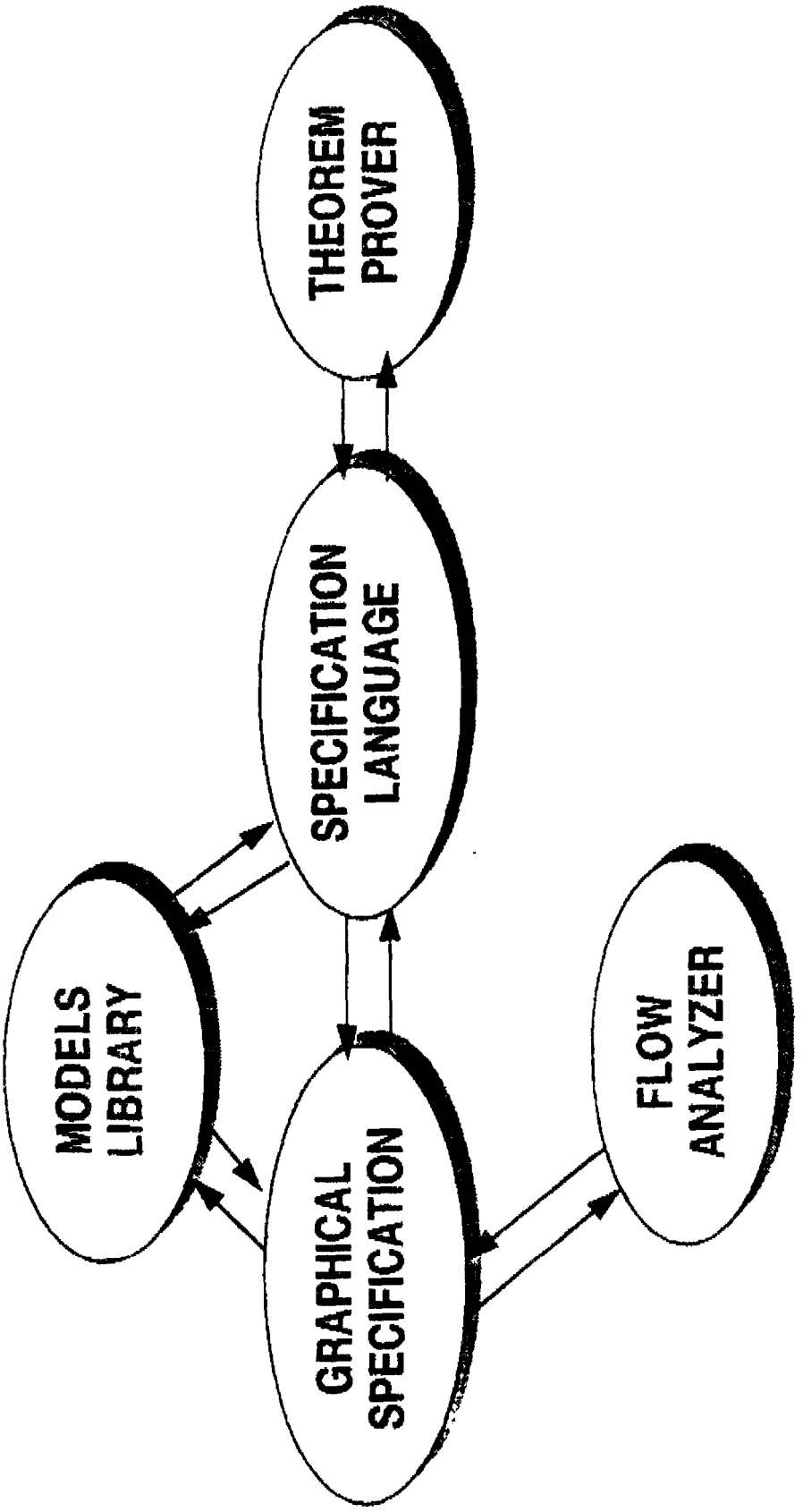
TOP-BOTTOM VERIFICATION



WHAT IS ROMULUS?

ROMULUS IS A WORKSTATION-BASED, TRUSTED SYSTEM DESIGN ENVIRONMENT TO MODEL, ANALYZE, & VERIFY THE SECURITY PROPERTIES OF TRUSTED, DISTRIBUTED COMPUTER SYSTEMS

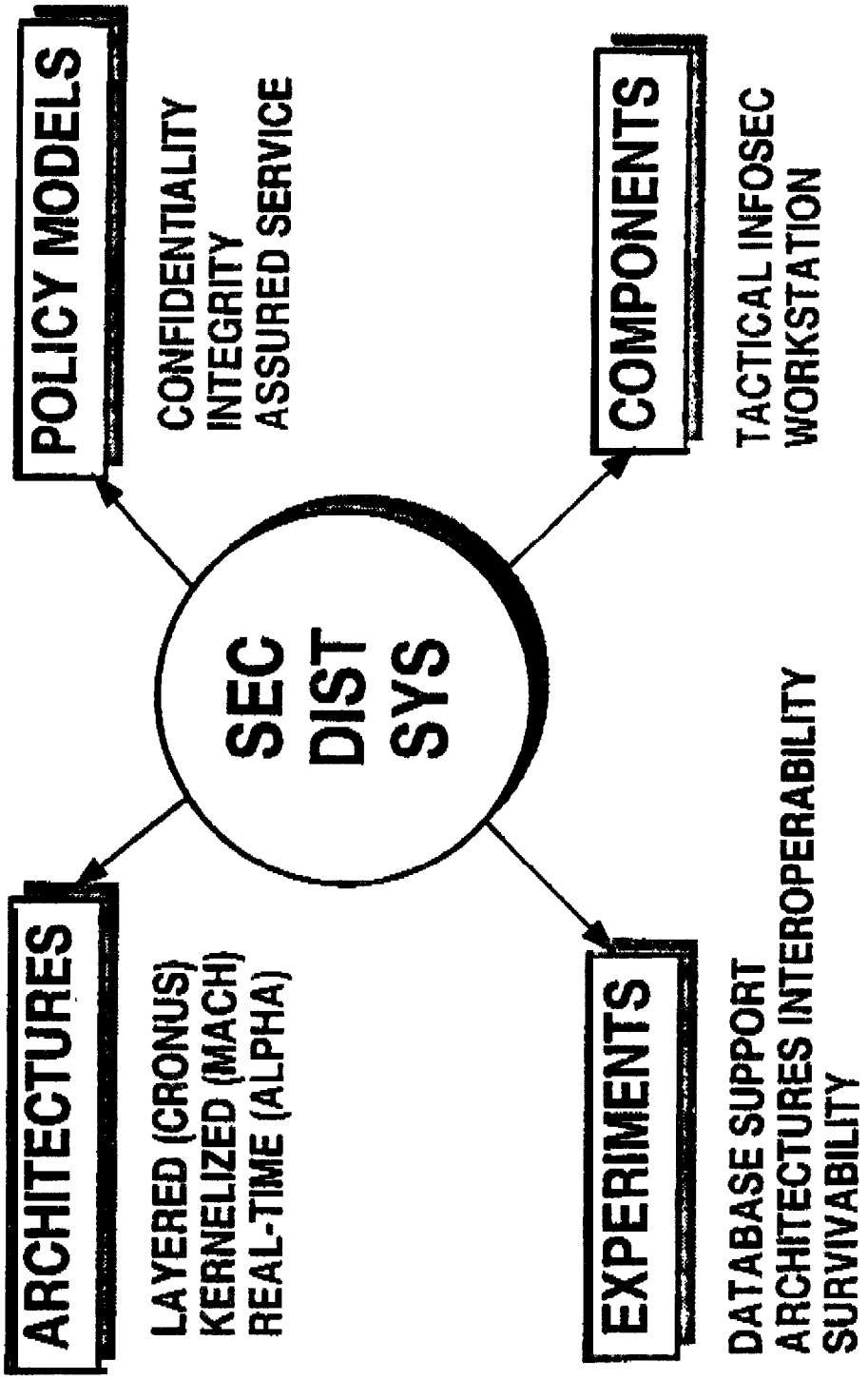
COMPONENTS OF ROMULUS



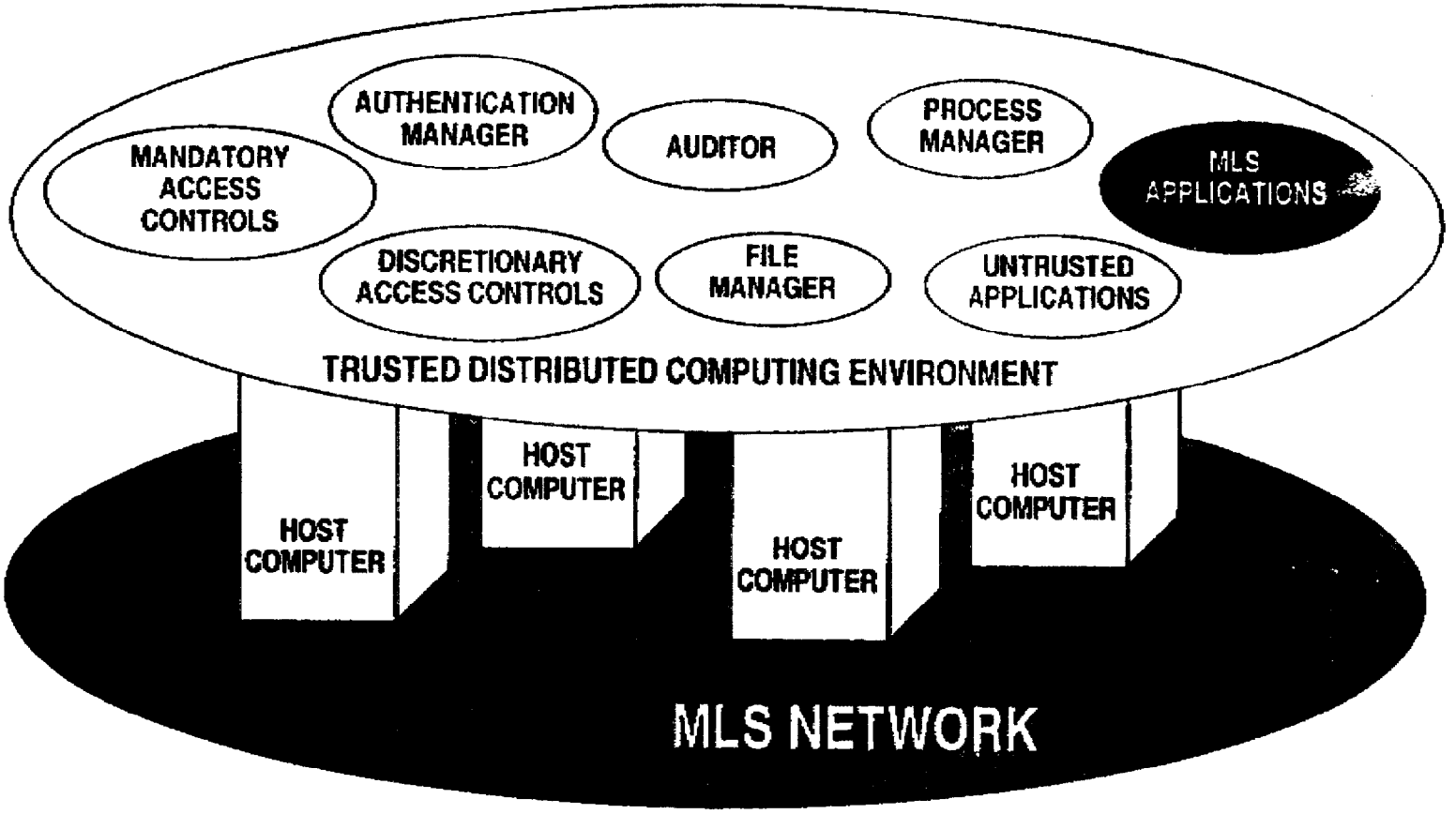
SYSTEM DESIGN WITH ROMULUS

ROMULUS EXTENSIONS

- REQUIREMENTS TOOL INTEGRATION
- ROMULUS/PENELOPE INTEGRATION
- ENHANCED MODELING SUPPORT


POLICY MODELS
CONFIDENTIALITY
INTEGRITY
ASSURED SERVICE
COMPONENTS
TACTICAL INFOSEC
WORKSTATION
SEC
DIST
SYS
ARCHITECTURES
LAYERED (CRONUS)
KERNELIZED (MACH)
REAL-TIME (ALPHA)
EXPERIMENTS
DATABASE SUPPORT
ARCHITECTURES INTEROPERABILITY
SURVIVABILITY

MLS DISTRIBUTED OPERATING SYSTEM



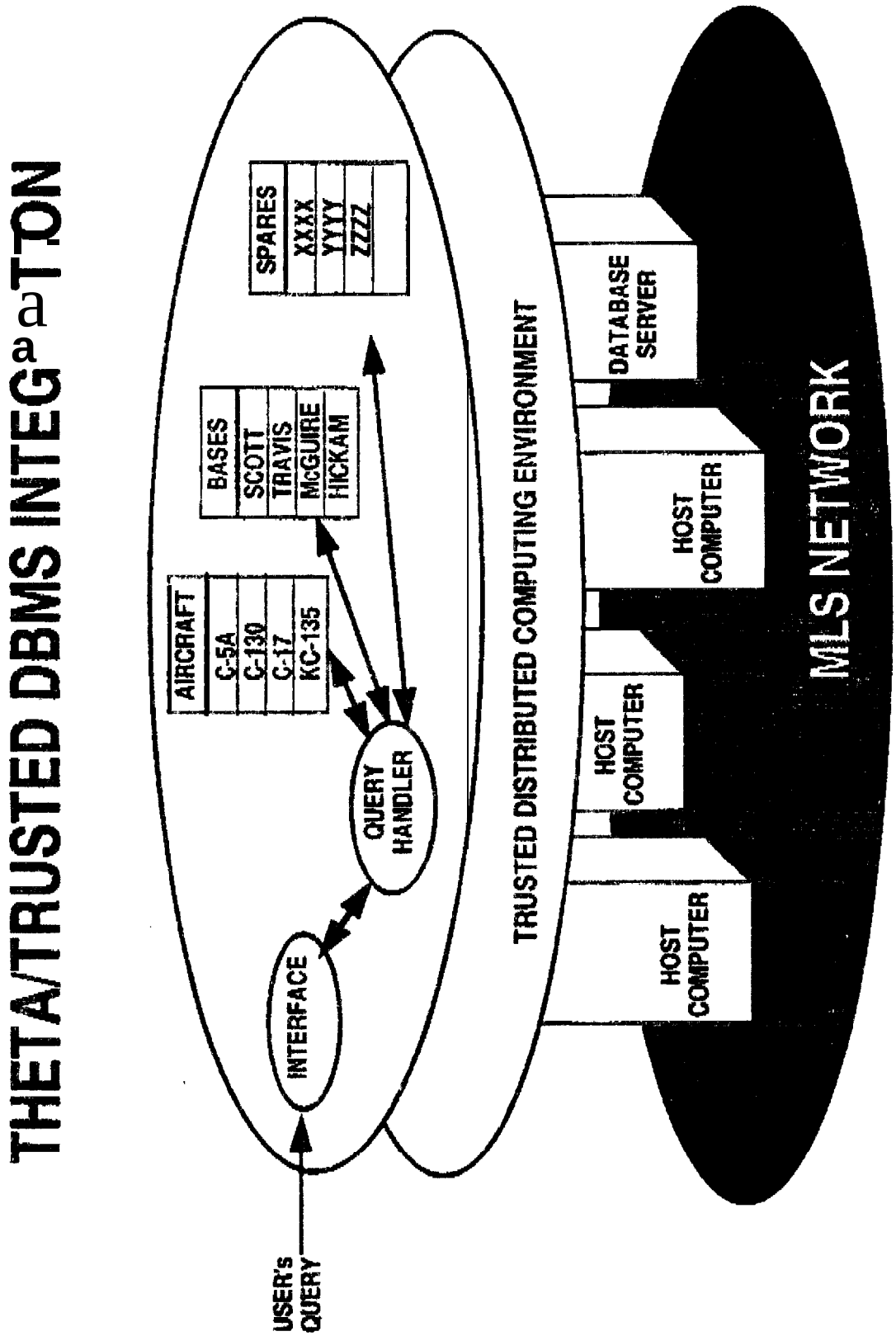
KAMAN ES-SYR ID:315-472-7241 OCT 11'93 12:19 No.002 P.14

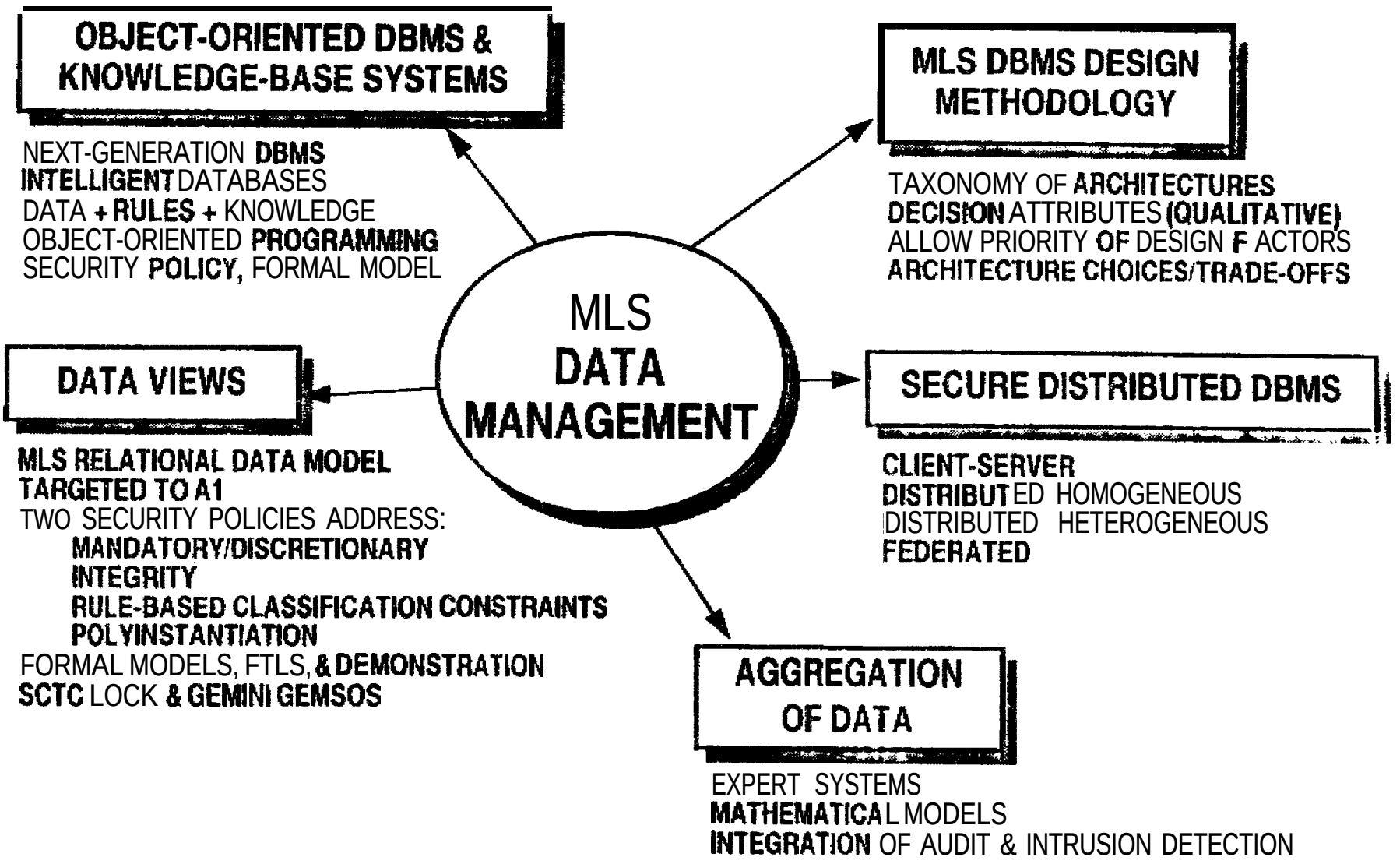
THETA PROGRAM-HISTORY

- ROME LAB SUPPORT FROM 1985
- CONCEPT EXPLORATION PHASE ("PHASE I"):
  - BBN/ORA, 198547
  - STUDY DISTRIBUTED SECURITY; FORMULATE POLICY
  - DESIGN A SECURE DISTRIBUTED OS
  - CARRY OUT AI-LEVEL VERIFICATION FOR ASSURANCE
- DEMONSTRATION/VALIDATION PHASE ("PHASE II"):
  - ORA/BBN, 1988-92
  - DETAILED DESIGN & POLICY BASED ON PHASE I WORK
  - IMPLEMENT PROTOTYPE
  - B3-LEVEL DESIGN & ASSURANCE

AMAN SCIENCES-SYR ID:315-472-7241 OCT 11'93 2. No. 002

THETA/TRUSTED DBMS INTEGRATION





KAMAN SCIENCES-SYR ID:315-472-7241 OCT 11 '93 12:20 No.002 P.17

TRUSTED DATABASE FRONT-END

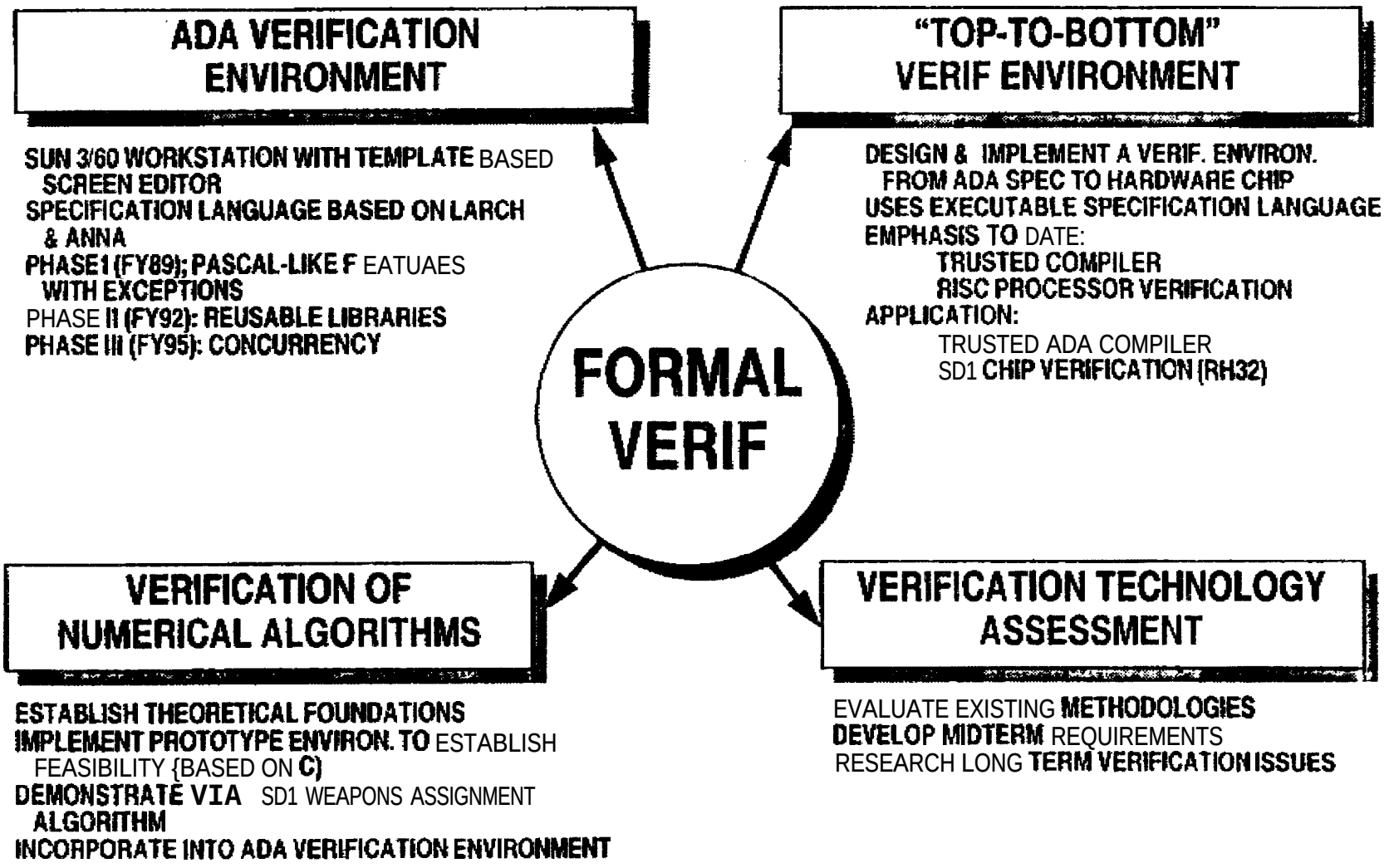
OBJECTIVE:

- DEVELOP & DEMONSTRATE TRUSTED DBMS FRONT-END CAPABILITIES TO SUPPORT
  - MULTILEVEL WORKSTATION INTERFACE
  - MULTILEVEL OUTPUT TECHNOLOGY
  - PRESENTATION TECHNOLOGY
  - WINDOWING
  - TRUSTED DATA LABELS

PROGRAM REQUIREMENTS:

- BUILD TO AT LEAST CLASS B2
- TRUSTED SUBJECT APPROACH
- CLIENT-SERVER ARCHITECTURE

KAMAN SCIENCES-SYR ID:315-472-7241 OCT 11'93 12:21 No.002 P.18



KAMAN SCIENCES-SYR ID:315-472-7241 OCT 11'93 12:21 No.002 P.19

CERTIFICATION TECHNOLOGY

OBJECTIVE:

DEVELOP A METHODOLOGY & PROVIDE A SET OF TOOLS & TECHNIQUES TO SUPPORT THE SECURE SYSTEM ACCREDITATION/EVALUATION PROCESS & TO AID THE DETERMINATION OF THE DEGREE OF SECURITY PROVIDED BY AUTOMATED INFORMATION SYSTEMS

APPROACH:

- DEFINITIZE EXISTING CERTIFICATION PROCESS
- TAILOR PROCESS TO AIR FORCE NEEDS
- IDENTIFY AREAS AMENABLE TO AUTOMATION
- SURVEY EXISTING TOOLS/TECHNIQUES TO DETERMINE APPLICABILITY TO AIR FORCE SECURITY CERTIFICATION PROCESS
- DEVELOP A METHODOLOGY & NEW TOOLS & TECHNIQUES TO SUPPORT SYSTEM CERTIFICATION & LIFE CYCLE MANAGEMENT

KAMAN SCIENCES-SYR ID:315-472-7241 OCT 11'93 12:22 No.002 P.20

PROJECTED FY93 NEW STARTS

EFFORT TITLE	POINT OF CONTACT
TRUSTED DATABASE FRONT-END	JOSEPH GIORDANO/x2805
THETA/TRUSTED DBMS INTEGRATION	EMILIE J. SIARKIEWICZ/x3241
ROMULUS EXTENSIONS	JOHN C. FAUST/x3241